UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO,
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:	)	**Case No:** 2:24-MJ-131
	)	
The person of Matthew H. Nichols, DOB: 2/22/1979	)	
and the residence located at 13942 Westfall Road,	)	**Magistrate Judge:** VASCURA
Chillicothe, Ohio 45601, including any curtilage, detached	)	
buildings and garages, and any computers or digital media	)	
located therein/thereon.	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeremy Lindauer (Your Affiant), a Special Agent with the Federal Bureau of Investigation (FBI), Athens Resident Agency, being first duly sworn, hereby depose and state:

EDUCATION, TRAINING AND EXPERIENCE

1. I am a Special Agent (SA) with the Federal Bureau of Investigations (FBI) and have been since September of 2015. I am currently assigned to the Resident Agency in Athens, Ohio.
2. Prior to joining the FBI, I worked as a patrol officer for the Fishers Police Department in Fishers, Indiana, between 2008 and 2015. While there, I received training and experience in conducting many types of criminal investigations, including crimes against children. I was promoted to Field Training Officer for the department prior to leaving to accept a position as Special Agent for the FBI in 2015. Within the FBI, I was first assigned to the Joint Terrorism Task Force in New York City, where I conducted and assisted in complex terrorism investigations across the globe. I was transferred to the Athens Resident Agency in September of 2020, where my responsibilities expanded to include investigating criminal violations relating to child exploitation and child pornography violations, including the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A.
3. As a federal agent, I am authorized to investigate violations of laws of the United States and have the authority to execute warrants issued under the authority of the United States. As part of my daily duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography, including the illegal production, distribution, receipt and

possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A.

PURPOSE OF THE AFFIDAVIT

4. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachments A, B, and C** of this Affidavit. The facts and statements set forth in this affidavit are based on my knowledge, experience, and investigation, as well as the knowledge, experience, and investigative findings of others with whom I have had communications about this investigation, including other law enforcement officers and agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause for a search warrant for the person of Matthew H. Nichols, DOB: 2/22/1979 (the **SUBJECT PERSON**) and the residence located at 13942 Westfall Rd, Chillicothe, Ohio, 45601 (the **SUBJECT PREMISES**). I have not omitted any facts that would negate probable cause.
5. The **SUBJECT PERSON** and **SUBJECT PREMISES** to be searched are more particularly described in Attachment A and Attachment B respectively, for the items specified in Attachment C, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, – advertising/solicitation for/or, and distribution and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter "child pornography"), sexual exploitation of a minor, distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the **SUBJECT PERSON** and the entire **SUBJECT PREMISES**, including the residential dwelling, curtilage, detached buildings and storage units, for any computers, cellular "smart" phones and/or mobile computing device or digital media located thereon/therein, and to thereafter seize and examine any such device that is recovered from the **SUBJECT PERSON** or **SUBJECT PREMISES**, for items specified in Attachment C, and to seize all items listed in Attachment C as evidence, fruits, and instrumentalities of the above violations.

APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor

assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed; if that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce; or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

7. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.
8. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
9. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess

or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

10. The term "child pornography"[1], as it is used in 18 U.S.C. § 2252A, is defined pursuant to 18 U.S.C. § Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.
11. The term "sexually explicit conduct", as used in 18 U.S.C. §§ 2251 and 2252, is defined pursuant to 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to 18 U.S.C. § 2256(2)(B), "sexually explicit conduct" when used to define the term child pornography, also means "(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person."
12. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."

1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

13. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."
14. "Graphic" when used with respect to a depiction of sexually explicit conduct, means that viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10)).
15. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
16. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).
17. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
18. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
19. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include

[2] The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES, AND THE INTERNET

20. I know from my training and experience that computer hardware, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.
21. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.
22. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.
23. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such

computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

24. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

25. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile

device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses3 and other information both in computer data format and in written record format.

26. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

27. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until

it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

28. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

29. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

30. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment C.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

31. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be

processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a) Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b) Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

32. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU) as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

33. In addition, there is probable cause to believe that any computer or mobile computing device and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251, 2252, and 2252A, and should all be seized as such.

INVESTIGATION AND PROBABLE CAUSE

34. On September 6, 2023, an FBI Special Agent of the Honolulu (HI) Field Office was working in an undercover capacity (OCE) attempting to identify subjects involved in the online sexual exploitation of children. On this date, the OCE was utilizing a social media mobile

application (hereinafter referred to as the Mobile App[3]), which your affiant knows to be a secured messaging and communication portal. The OCE had entered into a group chat titled "Carnival Play, No Limits." Within that group, the OCE noticed a participant with vanity name "John Doe" and the username "@ohndoe09," who was later identified as Matthew H. Nichols, (the **SUBJECT PERSON**, herein after identified as **NICHOLS**).

35. On December 8, 2023, the OCE and **NICHOLS** engaged in conversations through direct messages via the Mobile App. During the conversation, **NICHOLS** indicated he had a sixteen-year-old daughter (herein referred to as Minor Victim One) and **NICHOLS** made statements to the OCE about how **NICHOLS** engaged in sexual acts with Minor Victim One. For example, **NICHOLS** made a comment within the Mobile App platform in reply to a video of child pornography that had been sent out by another user. The video depicted an overweight adult male laying on his back while engaging in sexual intercourse with what appears to be a pubescent minor female in which the female minor was straddling the male during the sexual intercourse. **NICHOLS** commented to the group "reminds me of me and my daughter. I will try to make a video this weekend and post it for you All to enjoy."
36. During a direct messaging conversation with OCE on or about December 8, 2023, **NICHOLS** stated "I will try my best to send you some pictures of my daughter this weekend as well." **NICHOLS** then distributed an image which depicted a fully nude pubescent female sitting down. A round mark near the minor female's right shoulder, similar to an old, healed cigarette burn or bullet wound, was visible in the photo. In the background of the photo, a purple, blue, and white blanket was also seen.
37. On or about December 10, 2023, **NICHOLS** distributed an unsolicited video in a direct message to OCE which contained an approximately nine second video depicting a fully nude pubescent female, laying on her back with her legs crossed. The focus of the camera started at the minor female's feet and slowly panned up her body, to her exposed vagina and breasts. The minor female's face was covered with a purple, blue, and white blanket, similar to the one identified in the previous image. In the last few seconds of the video, the camera zoomed in on the minor female's nude vagina. In the background, a female voice is heard stating "Hey Matt, get your ass out here."

[3] The name of the application used by the OCE has been redacted for purposes of protecting the integrity of the investigation into this mobile application which is often used to facilitate the trading of child pornography.

38. On or about December 9, 2023, **NICHOLS** a video to the "Carnival Play, No Limits" chat group, with a caption that read "My daughter." The video, approximately twelve seconds in length, depicted a minor female's laying down on her back with a white pillow covering her face, wearing a pink and gray shirt, with her shirt opened and her breasts exposed. An adult male's left hand is seen on her chest and wearing a dark colored ring on his ring finger, and has what appeared to be a skin mark on his hand. The video depicted the male rubbing the minor female's breasts with his left hand and playing with her nipple.
39. After distributing the video and within the ensuing conversation **NICHOLS** made the following statements: "Me my wife and daughter just have to wait for a few for my mother in law to leave...," "Yes me my wife and daughter all 3 Play together...," "No my wife is not her mother....," and "I have never used my daughter as just some fuck toy. We actually love each other."
40. The OCE noted that **NICHOLS** then distributed to the group the same nine second video described above that he had shared with OCE on December 10, 2023. **NICHOLS** then distributed an additional video, approximately thirteen seconds in length, which depicted a topless pubescent girl, standing up next to a bed wearing white underwear, and an adult male's left hand grabbing her breast. The camera then moved away from the minor female, and the minor female cupped her own breast and stood there with her hand on her hip. There was a round mark near the minor female's right shoulder similar to the mark identified in the previous image. The minor female's face was not shown in the video.
41. The OCE further reviewed another video posted by **NICHOLS** to the "Carnival Play, No Limits" chat group. The video was of two females masturbating in bed. The OCE believed one of the females in the video was Minor Victim One, based on the similar body shape and size compared to the other videos of who **NICHOLS** claimed was his daughter. It was implied that the other female in the video with Minor Victim One was the wife of **NICHOLS** based on the comments he had made in the group about all three of them "playing together." In the video, pillows were covering both of the females' heads as to conceal their identity.[4]

[4] The OCE personally observed the video within the chat but was not able to capture a copy of the video before it was removed from the Mobile App. The FBI does not possess a copy of this video, and the captioned description is based on the recollection of the FBI OCE.

42. Private communications between the OCE and **NICHOLS** continued and on or about December 15, 2023, when **NICHOLS** made the following statements.

- In response to a question about how often he engages in sexual activity with his daughter he stated, "We get to just about every weekend."

- In response to a question about how his wife got onboard with this activity **NICHOLS** stated, "My daughter did that. My wife is not my daughters mother. My wife is only 8 years older than my daughter. She [referring to his daughter again] started talking about being with a nother girl. And one night she talks my wife into tieing me to the bed so they could tickle me. And one thing led to another. No I didn't ask her to do that. But she wanted to. Always knew that I liked to be with 2 girls. And my daughter loves me so much that she wanted to make it happen for me."

43. Later that same date, **NICHOLS** distributed an approximately ten second video to the OCE in their private chat which depicted a fully nude pubescent girl, sitting on top of a nude adult male. The camera angle zoomed in on the female minor's vagina, which was simulating sexual intercourse with the adult male. The camera panned up the female minor's body, and the same round mark from the previously described image was visible next to the female minor's right shoulder. The female minor's left hand was covering her own face, which was not visible. The OCE noted that this video was similar to the video **NICHOLS** replied to on December 8, 2023 in the "Carnival Play, No Limits" group chat in which he stated he would "try to make a video this weekend and post it for you All to enjoy."

44. On or about December 13, 2023, the FBI reached out to the Legal Attaché United States Embassy in Bern, Switzerland, to request data for the Mobile App account associated with John Doe, @ohndoe09. On December 14, 2023, SWISS FEDPOL responded to a request for information related to the account. In response, the following information was provided, related to John Doe with handle @ohndoe09:

Identification:	fc70164a-de7a-4f76-8403-81f8a678364f
Name/First Name:	John Doe
E-Mail:	starjammer08@skiff.com

45. As part of the investigation, the FBI reached out to skiff.com and learned they do not keep records relating to their users and registered email addresses.

46. On December 18, 2023, a federal court order was served to Google, Inc for any account associated with starjammer08@skiff.com email address, which was the email address

associated with Mobile App user @ohndoe09, display name: John Doe. On December 20, 2023 Google responded with "No Records Found."

47. Further open-source checks revealed that the email address starjammer08@skiff.com, with username "starjammer08" had an account Kik account. On December 20, 2023, an administrative subpoena was served to Kik for user "starjammer08". Kik provided results which included several IP addresses ranging from several dates during the span of on or about December 1, 2023, through on or about December 18, 2023. The information provided by Kik identified which IP address that the user was likely connected to, which included locations in Cincinnati, Cleveland, Washington Courthouse, Willoughby, and Columbus, Ohio, as well as Jeannette, Greensburg, Willoughby, and Delmont, Pennsylvania.
48. On December 20, 2023, an administrative subpoena was served to Charter Communications for IP Address: 98.102.141.194 on 2023-12-13 at 19:09 UTC which was one of the IP addresses received from Kik. On January 2, 2023, Charter Communications provided the following results:

Subscriber Name:	New Sabina Industries
Service Address:	12555 US Highway 22E Sabina, OH 45169
Email:	Jennifer.Porter@nsna.com
User Phone:	931-584-2433

49. On January 18, 2024 an administrative subpoena was served to Verizon for the following IP's that were identified in the Kik account as well: 174.203.134.45 port: 8567 on 2023/12/19 at 21:30:14 UTC, 174.203.134.45 port: 10264 on 2023/12/17 at 05:48:32 UTC, and 174.207.100.232 port: 4279 on 2023/12/16 at 04:05:06 UTC.
50. On January 24, 2024, Verizon provided results from the IP address located in the Kik account, which identified the telephone number (740) 656-0530 (hereinafter referred to as X0530). Your affiant learned that the X0530 number was sold to TracFone.
51. On February 5, 2024, an administrative subpoena was served to TracFone for X0530.
52. On February 29, 2024 Tracfone provided responsive results for the X0530 request which indicated that telephone number was associated with Electronic Serial Number (ESN) 016053004800406.

53. On March 1, 2024, an administrative subpoena was submitted to Google, Inc. for information pertaining to ESN/IMEI: 016053004800406[5] as received from TracFone.

54. On March 1, 2023, Google provided responsive results indicating the subscriber information and user was matthewnichols74@gmail.com with a recovery SMS telephone number of (740) 656-0530. Additional records identified IP activity between December 2, 2023 and February 29, 2024. Google also provided records for the Device and Account attributed to the ESN/IMEI number as an Android ID: 4428393767779166643; IMEI: 016053004800406; Serial Number: Jetta_TF:RK8LZPXGMRZ5SK69, and User:matthewnichols74@gmail.com. Your affiant would note that the IP activity for the account attributed to the **SUBJECT PERSON** falls within the OCE communications that took place with "Minor Victim One."

55. Law enforcement then did a check for the email address matthewnichols74@gmail.com in law enforcement databases and discovered a connection to Matthew H. **NICHOLS** of Chillicothe, Ohio. Further open-source searches via social media accounts related to **NICHOLS** revealed that **NICHOLS** had recently married Charity Nichols, DOB: (herein after **CHARITY**) in June of 2023. Your affiant observed a photograph posted to **NICHOLS'** Facebook page depicting **NICHOLS** and **CHARITY** posing with a marriage license, alongside a minor female who appeared to be approximately sixteen years old. Additional open-source research into the minor female revealed that female to be Minor Victim One as seen in the videos and images shared by **NICHOLS** to the OCE and Mobile App group. More specifically, this determination was made by matching the general appearance of Minor Victim One in both the social media content as well as the content distributed by **NICHOLS**, both of which depict Minor Victim One with a round mark near her right shoulder.

56. Furthermore, your affiant obtained a report from the Ohio Department of Jobs and Family Services dated September 16, 2023 pertaining to Minor Victim One and her family. The report listed Minor Victim One's full name and date of birth as April 17, 2008. At the time **NICHOLS** distributed the videos and images of Minor Victim, she would have been

[5] The IMEI and ESN are similar in that they both are used to uniquely identify a mobile device. ESN was used by CDMA carriers such as Sprint and Verizon, and the IMEI is used by GSM carriers such as T-Mobile and AT&T. Providers such as Google use the terms interchangeably.

approximately fifteen years of age. That same report verified that **NICHOLS** was the parent of Minor Victim One. In that same report, **NICHOLS** phone number is listed as the X0530.

57. In an attempt to locate **NICHOLS** and determine his current residence, a deputy from the Ross County Sheriff's Office went to the **SUBJECT PREMISES** on or about March 3, 2024 and spoke to a woman named Dorothea, who lived at that address and told the deputy that **NICHOLS** and **CHARITY** both lived at that address but were not home at the time of the contact. Additionally, a search of law enforcement databases revealed that **CHARITY's** current address was the **SUBJECT PREMISES**. Finally, on March 5, 2024 a Special Agent with the FBI drove by the **SUBJECT PREMISES** and observed an orange SUV bearing Ohio license plate HZJ2280. A search of Ohio BMV records revealed that vehicle was registered to **CHARITY.**

58. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, are located on/in the **SUBJECT PREMISES** and **SUBJECT PERSON**. Therefore, I respectfully request that this Court issue search warrants for the locations described in **Attachments A and B**, authorizing the seizure and search of the items described in **Attachment C**.

SEARCH METHODOLOGY TO BE EMPLOYED

59. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

    a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in Attachment C;

    b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment C;

    c. Surveying various files, directories and the individual files they contain;

    d. Opening files in order to determine their contents;

    e. Scanning storage areas;

f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment C; and/or

g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment C.

COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

60. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in children and who produce, distribute, and receive child pornography:

a) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c) Those who have a sexual interest in children and who produce, distribute, and receive child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and

video tapes for many years. More recently, however, it has become more common for people who have a sexual interest in children to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

d) Likewise, those who have a sexual interest in children and who produce, distribute, and receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e) Those who have a sexual interest in children and who produce, distribute, and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and sometimes maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f) Those who have a sexual interest in children and who produce, distribute, and receive child pornography rarely are able to abstain from engaging in sexual exploitation of children or child pornography activities for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

61. When images and videos of child pornography are produced and stored on computers and related digital media, forensic evidence of the production, distribution, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

62. Based upon the conduct of individuals involved in seeking/soliciting, receiving, distributing, and/or collecting child pornography set forth in the above paragraphs, and the

facts learned during the investigation in this case, namely, that **NICHOLS** was bragging about having a sexual relationship with his minor daughter and sending content to a social media group dedicated to the sexual exploitation of a minor, your affiant has reason to believe that **SUBJECT PERSON** has a sexual interest in minors and has prdued, viewed or sought out visual depictions of minors engaged in sexually explicit conduct utilizing an internet-capable device, which may include a cellular phone that **SUBJECT PERSON** likely carries on his person. Your affiant therefore submits that there is probable cause to believe the evidence of the offenses of 18 U.S.C. §§ 2251, 2252, and 2252A, – advertising/solicitation for/or, and distribution and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter "child pornography"), sexual exploitation of a minor, distribution, transmission, receipt, and/or possession of child pornography, will be located on the **SUBJECT PERSON** and/or in the **SUBJECT PREMISES** and any digital device that may be found on/in the **SUBJECT PERSON** or the **SUBJECT PREMISES.**

CONCLUSION

63. Based on all the forgoing factual information, there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, and 2252A, – advertising/solicitation for/or, and distribution and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter "child pornography"), sexual exploitation of a minor, distribution, transmission, receipt, and/or possession of child pornography, and evidence of those violations is located on the person described in **Attachment A** and in the residence described in **Attachment B.** Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in **Attachment C.**

Jeremy Lindauer
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 6th day of March, 2024.

Chelsey M Vascura

The Honorable Chelsey M. Vascura
United States Magistrate Judge
United States District Court
Southern District of Ohio